UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/942,994	08/31/2001	Takuya Morishita	Q66052	9297

7590 09/29/2006

SUGHRUE, MION, ZINN, MACPEAK & SEAS
2100 Pennsylvania Avenue, N.W.
Washington, DC 20037

EXAMINER	
HA, LEYNNA A	
ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 09/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/942,994	**Applicant(s)** MORISHITA, TAKUYA	
	Examiner LEYNNA T. HA	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 July 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15 and 20-22* is/are pending in the application.

4a) Of the above claim(s) *16-19* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15 and 20-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-15 and 20-22 are pending.

2. Claims 16-19 have been cancelled by applicant. Thus, claim 18 was previously rejected under 35 U.S.C. 101, is now withdrawn.

3. This is a Final rejection necessitated by new grounds of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-4, 6-9, 11-14, and 20-22 are rejected under 35 U.S.C. 102(e) as being anticipated by Ginter, et al. (US 5,910,987).

As per claim 1:

Ginter discloses a system for decrypting an encrypted computer program including at least one first block and a plurality of second blocks in sequence, the system comprising:

means for generating a first cipher key **[col.190, lines 32-42]** from the at least one first block of the encrypted computer program; **[col.11, lines 58-64 and col.126, lines 47-64; Ginter discloses content portions is divided into portions called data blocks where security will be enhanced by using at least one key block for each data block.]**

means for performing a first decryption on each of the plurality of second blocks of the encrypted computer program **[col.128, lines 34-43 and col.163, lines 23-25]** with said first cipher key which is generated from the at least one first block; **[col.31, lines 55-57 and col.63, lines 53-55]**

means for performing a second decryption on each of the plurality of second blocks, wherein for each of said plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key. **[col.149, lines 52-57 and col.190, lines 3-28]**

As per claim 2: See col.31, lines 45-46 (Ginter suggests encrypting in part or in whole, so when in part there is at least one block that is not encrypted.); discussing wherein said at least one a first block is not encrypted.

As per claim 3: See col.149, lines 52-57 and col.163, lines 23-25; discussing plurality of second blocks are encrypted at least with said first cipher key prior being decrypted.

As per claim 4: See col.127, lines 17-22 and col.128, lines 34-43; discussing at least one of said plurality of second blocks is encrypted with said second cipher key prior being decrypted.

As per claim 6:

Ginter discloses a method for decrypting an encrypted computer program including at least one first block and a plurality of second blocks in sequence, the method comprising the steps of:

generating a first cipher key **[col.190, lines 32-42]** from the at least one first block of the encrypted computer program; **[col.11, lines 58-64 and col.126, lines 47-64; Ginter discloses content portions is divided into portions called data blocks where security will be enhanced by using at least one key block for each data block.]**

performing a first decryption on each of the plurality of second blocks of the encrypted computer program **[col.128, lines 34-43 and col.163, lines 23-25]** with said first cipher key which is generated from the at least one first block; **[col.31, lines 55-57 and col.63, lines 53-55]**

performing a second decryption of the plurality of second blocks, wherein for each of said plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key. **[col.149, lines 52-57 and col.190, lines 3-28]**

As per claim 7: See col.31, lines 45-46 (Ginter suggests encrypting in part or in whole, so when in part there is at least one block that is not encrypted.); discussing said at least one first block is not encrypted.

As per claim 8: See col.149, lines 52-57 and col.163, lines 23-25; discussing plurality of second blocks are encrypted at least with said first cipher key prior being decrypted.

As per claim 9: See col.127, lines 17-22 and col.128, lines 34-43; discussing at least one of said plurality of second blocks is encrypted with said second cipher key prior being decrypted.

As per claim 11:

Ginter discloses a computer program product embodied on a computer-readable medium and comprising code that, when executed, causes a computer to perform a method for decrypting an encrypted computer program including at least one first block and a plurality of second blocks in sequence, said method comprising the steps of:

generating a first cipher key from at least one first block **[col.190, lines 32-42]** of the encrypted computer program; **[col.11, lines 58-64 and col.126, lines 47-64; Ginter discloses content portions is divided into portions called data blocks where security will be enhanced by using at least one key block for each data block.]**

performing a first decryption on each of the plurality **[col.128, lines 34-43 and col.163, lines 23-25]** of second blocks of the encrypted computer program with said first cipher key; and **[col.31, lines 55-57 and col.63, lines 53-55]**

performing a second decryption of the plurality of second blocks, wherein for each of said plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key. **[col.149, lines 52-57 and col.190, lines 3-28]**

As per claim 12: See col.31, lines 45-46 (Ginter suggests encrypting in part or in whole, so when in part there is at least one block that is not

encrypted.); discussing said at least one block is not encrypted.

As per claim 13: See col.149, lines 52-57 and col.163, lines 23-25; discussing plurality of second blocks are encrypted at least with said first cipher key prior being decrypted.

As per claim 14: See col.127, lines 17-22 and col.128, lines 34-43; discussing at least one of said plurality of second blocks is encrypted with said second cipher key prior being decrypted.

As per claims 16-19: cancelled

As per claim 20: See col.3, lines 59-61; discussing means for performing the second decryption of the plurality of second blocks executes the second decryption faster than said means for performing the first decryption of the plurality of second blocks.

As per claim 21: See col.3, lines 59-61; discussing means for performing the second decryption of the plurality of second blocks executes the second decryption faster than said means for performing the first decryption of the plurality of second blocks.

As per claim 22: See col.3, lines 59-61; discussing means for performing the second decryption of the plurality of second blocks executes the second decryption faster than said means for performing the first decryption of the plurality of second blocks.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 5, 10, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginter, et al. (US 5,910,987) in further view of Lotspiech, et al. (US 6,118,873).

As per claim 5:

Ginter discloses a system for decrypting an encrypted computer program including at least one first block and a plurality of second blocks in sequence, the system comprising means for generating a first cipher key [col.190, lines 32-42] from the at least one first block of the encrypted computer program [col.11, lines 58-61 col.126, lines 47-64] Ginter discloses content portions is divided into portions called data blocks where security will be enhanced by using at least one key block for each data block. Further, Ginter discloses performing a first decryption on each of the plurality of second blocks of the encrypted computer program [col.128, lines 34-43 and col.163, lines 23-25] with said first cipher key which is generated from the at least one first block [col.31, lines 55-57 and col.63, lines 53-55], and performing a second decryption on each of the plurality of second blocks, wherein for each of said plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key [col.149, lines 52-57 and col.190, lines 3-28]. However, Ginter did not discuss in details the means for determining whether or not the encrypted computer program is analyzed and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed.

Lotspiech, et al., discloses a system for encrypting broadcast programs running on plural devices and to determine whether the devices running the programs have been compromised. Lotspiech discusses means for determining whether or not the encrypted computer program is analyzed to determine whether any devices have been compromised **(col.6, lines 52-54 and col.8, lines 16-35)** and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed **(col.7, lines 26-31 and col.8, lines 24-26)**.

It would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teachings of Ginter with the means for determining whether or not the encrypted computer program is analyzed and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed as taught by Lotspiech because by analyzing the program determines whether any devices have been compromised and to decrypt the dummy blocks rather than the plurality of second blocks so that it prevents the unwanted and unauthorized user or device from obtaining the real key thereby to the actual program.

As per claim 10:

Ginter discloses a system for decrypting an encrypted computer program including at least one first block and a plurality of second blocks in sequence, the system comprising means for generating a first cipher key [col.190, lines 32-42] from the at least one first block of the encrypted computer program [col.11, lines 58-61 col.126, lines 47-64] Ginter discloses content portions is divided into portions called data blocks where security will be enhanced by using at least one key block for each data block. Further, Ginter discloses performing a first decryption on each of the plurality of second blocks of the encrypted computer program [col.128, lines 34-43 and col.163, lines 23-25] with said first cipher key which is generated from the at least one first block [col.31, lines 55-57 and col.63, lines 53-55], and performing a second decryption on each of the plurality of second blocks, wherein for each of said plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key [col.149, lines 52-57 and col.190, lines 3-28]. However, Ginter did not discuss in details the means for determining whether or not the encrypted computer program is analyzed and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed.

Lotspiech, et al., discloses a system for encrypting broadcast programs running on plural devices and to determine whether the devices running the programs have been compromised. Lotspiech discusses means for determining whether or not the encrypted computer program is analyzed to determine whether any devices have been compromised **(col.6, lines 52-54 and col.8, lines 16-35)** and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed **(col.7, lines 26-31 and col.8, lines 24-26)**.

It would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teachings of Ginter with the means for determining whether or not the encrypted computer program is analyzed and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed as taught by Lotspiech because by analyzing the program determines whether any devices have been compromised and to decrypt the dummy blocks rather than the plurality of second blocks so that it prevents the unwanted and unauthorized user or device from obtaining the real key thereby to the actual program.

As per claim 15:

Ginter discloses a system for decrypting an encrypted computer program including at least one first block and a plurality of second blocks in sequence, the system comprising means for generating a first cipher key [col.190, lines 32-42] from the at least one first block of the encrypted computer program [col.11, lines 58-61 col.126, lines 47-64] Ginter discloses content portions is divided into portions called data blocks where security will be enhanced by using at least one key block for each data block. Further, Ginter discloses performing a first decryption on each of the plurality of second blocks of the encrypted computer program [col.128, lines 34-43 and col.163, lines 23-25] with said first cipher key which is generated from the at least one first block [col.31, lines 55-57 and col.63, lines 53-55], and performing a second decryption on each of the plurality of second blocks, wherein for each of said plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key [col.149, lines 52-57 and col.190, lines 3-28]. However, Ginter did not discuss in details the means for determining whether or not the encrypted computer program is analyzed and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed.

Lotspiech, et al., discloses a system for encrypting broadcast programs running on plural devices and to determine whether the devices running the programs have been compromised. Lotspiech discusses means for determining whether or not the encrypted computer program is analyzed to determine whether any devices have been compromised **(col.6, lines 52-54 and col.8, lines 16-35)** and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed **(col.7, lines 26-31 and col.8, lines 24-26)**.

It would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teachings of Ginter with the means for determining whether or not the encrypted computer program is analyzed and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed as taught by Lotspiech because by analyzing the program determines whether any devices have been compromised and to decrypt the dummy blocks rather than the plurality of second blocks so that it prevents the unwanted and unauthorized user or device from obtaining the real key thereby to the actual program.

Response to Arguments

6. Applicant's arguments with respect to claims 1-15 and 20-22 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

LHa